Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2000 Proceedings

Americas Conference on Information Systems (AMCIS)

2000

BS7799: A Suitable Model for Information Security Management

Haiwen Li
Southampton Institute, haiwen.li@solent.ac.uk

Graham King
Southampton Institute

Margaret Ross
Southampton Institute

Geoff Staples
Southampton Institute

BS7799: A Suitable Model for Information Security Management

Haiwen Li, Graham King, Margaret Ross, Geoff Staples, Haiwen.Li@solent.ac.uk
Systems Engineering Research Centre, Southampton Institute, UK

Abstract

The world is changing rapidly as technology marches forward and the modern business world expands to take advantage of the new technology. Security is seen as fundamental to rapid changing E-business. To satisfy the urgent need for security on the Internet, organisations need to face these challenges and need a suitable management model for information security management.

This paper presents the current foundation of information security standard and analyses the framework of BS7799 British information security model. It describes the basic properties of the important security management processes: security policy, security standards, access control, security architecture. It provides an opportunity for security manager to gain security management knowledge and recognise the important procedures and mechanisms to improve the process of information security management.

1. Introduction

The Internet is growing up and E-commerce will revolutionise business, customers will be offered new and exciting services, businesses will be run more efficiently. New technologies are being developed and improved every day. Internet is no longer a playing field for academic research and related user groups, but an area where significant amounts of money can be made or lost. A business world that is made up of E-commerce, distributed computing, global networking connections. New ways of doing business do not come without new risks, in fact, business and computer system security problems have happened frequently. For example, there has been theft of money and information from the Internet; computer systems have crashed through viruses in many organisations throughout the world; security gaps could enable a hacker to browse user's bank details.

In order to make information system safe, governments have published new laws to protect privacy and the ownership of information. Organisations have also developed a host of security measures, like passwords and cryptography, but many governments and organisations run into problems when they try to cross national boundaries. There is no global law.

There are a growing number of guides available, providing instructions on how to secure corporate information assets when connected to the Internet. Professional security organisations have also published practical recommendations (e.g. the Computer Security Institute, 1997). The internet is also a rich source of information: organisations such as the National Institute of Standards and Technology (NIST) in the US and the national computing centre in the UK. They provide information on security products, advice on policy to help companies across the globe (Sanderson and Forcht, 1996).

The British Standards Institution published the Information Security Management Standard BS7799 in 1995, it has recently been adopted by Australia and New Zealand. It provides an authoritative statement on the organisational need for information security, and the procedures to be adopted for baseline security. This paper presents a comprehensive information security model BS7799 and describes the basic properties of the most important security processes, to provide a common, best practice guidance to enable an organisation to implement appropriate information security.

1.1 Background of BS7799

The origin of BS7799 goes back to the days of the UK Department of Trade and Industry's (DTI) Commercial Computer Security Centre (CCSC). Founded in May 1987, the CCSC had two major tasks. The first was to help vendors of IT security products by establishing a set of internationally recognised security evaluation criteria and an associated evaluation and certification scheme. The second task was to help users by producing a code of good security practice and resulted in a "Users Code of Practice" that was published in 1989. This was further developed by the National Computing Centre (NCC), and later a consortium of users, primarily drawn from British Industry, to ensure that the Code was both meaningful and practical from a user point of view. The final result was first published as a British Standard's guidance document PD 0003, *A code of practice for information security management*, and following a period of further public consultation recast as British Standard BS7799-1:1995. A second part BS7799-2: 1998 was added in February 1998.

The BS7799 technical committee also includes the following bodies: the BOC group plc; British Computer

Society; British Telecommunications plc; CCTA, Department of Trade and industry; Marks & Spencer plc; Midland bank plc; national building society, Prudential Assurance corporation; SEMA group consulting; Shell International Petroleum Co Ltd; Shell UK ltd, Unilerer plc. These companies and organisations are among the largest information systems users in the UK. First they are primarily users rather than developers or producers. More important is that, as users, they are all involved in business, which increasingly depends on networked services to their suppliers and customers.

There is a growing interest and take up of BS7799 in many other countries around the world, including Australia, Brazil, Denmark, Ireland, Japan, the Netherlands, New Zealand, Norway, Poland, South Africa, Switzerland and the USA. It is a clear benefit in having a common reference document for information security management. It enables mutual trust to be established between networked information systems and trading partners and provides a best formal management of these systems between users and services providers.

1.2 Objectives of BS7799

The purpose of the BS7799 methodology is to protect information from a wide range of threats in order to ensure business continuity and minimise business damage. BS7799 provides an opportunity for security managers to gain senior management recognition of the importance of procedures and mechanisms to enhance information security. The objectives of the BS7799 methodology are:

- To provide common, best practice guidance to enable an organisation to implement appropriate information security;
- To facilitate inter-company trading by providing confidence in the security of shared information;
- To ensure business continuity and minimise business damage;
- To help organisation to identify strength and weakness in the organisation's information security management processes;
- To plan improvement actions that support achievement of the organisation's goals;
- To enable organisations to implement and measure effective information security management practices and to provide confidence relating to third party access.

2. The BS7799 Architecture

The architecture has been designed to facilitate the assessment of an organisation's security management process, and to make judgements and recommendations regarding improvements to them. This is achieved by defining two parts of BS7799 for the baseline practices of information security management. Two parts of practices are:

BS7799 Part 1: 1995 is a standard code of practice and provide guidance on how to secure an information system. BS7799 part 1 provides guidance material to help companies to implement their own information security system. It provides 127 main headings to enable organisations to identify the security control which are appropriate to their particular business. It also identifies 10 key controls which are considered to be essential in providing effective information security.

BS7799 part 2: 1998 is a standard specification and specifies the management framework, objectives and control requirements for an Information Security Management System (ISMS). It defines a six-step process and specifies requirements for security controls to be implemented according to the needs of the individual organisation.

There is a certification scheme for BS7799, called "C:Cure" that works like ISO9000. The UK certificate scheme (C:Cure) is owned by the British Standards Institute (BSI/DISC) on behalf of the UK Department of Trade and Industry (DTI).

2.1 The Framework of BS7799 part 1

BS7799 part 1 provides guidance on best practice for information security management. Part 1 defines a set of control objectives together with a comprehensive set of supporting security control, it consists of ten major controls as shown in Figure 1. The areas of concern of the ten sections are:

(1) ***Information security policy:*** It provides management direction and support for information security.

(2) ***Security organisation:*** The recommendation of the security organisation section are concerned with the organisational structures, third party access and outsourcing. It includes information security co-ordination, allocation of information security responsibilities, authorisation process for IT facilities, specialist information security advice, co-operation between organisations, independent review of information security, security of third-party access. The need for a high-level management forum to ensure there is clear direction and visible management support for security initiatives.

(3) ***Assets, classification and control:*** It is to maintain appropriate protection of organisational assets and to ensure that information assets receive an appropriate level of protection. This section of standard can assist managers to decide what is important to the company by creating a formal scheme against which all working information can be classified. It includes accountability for assets, classification guidelines, and classification labelling.

(4) ***Personnel security:*** Personnel security is a major part of information security management. The objective of personnel security is to reduce the risks of human errors, theft, fraud or misuse of facilities. This section of the standard concerned with the following areas:

- security in job descriptions;
- recruitment screening;
- Confidentiality agreement;
- Information security education and training;
- Reporting of security incidents;
- Reporting of security incidents;
- Reporting of security weaknesses;
- Reporting of software malfunctions;
- Disciplinary process.

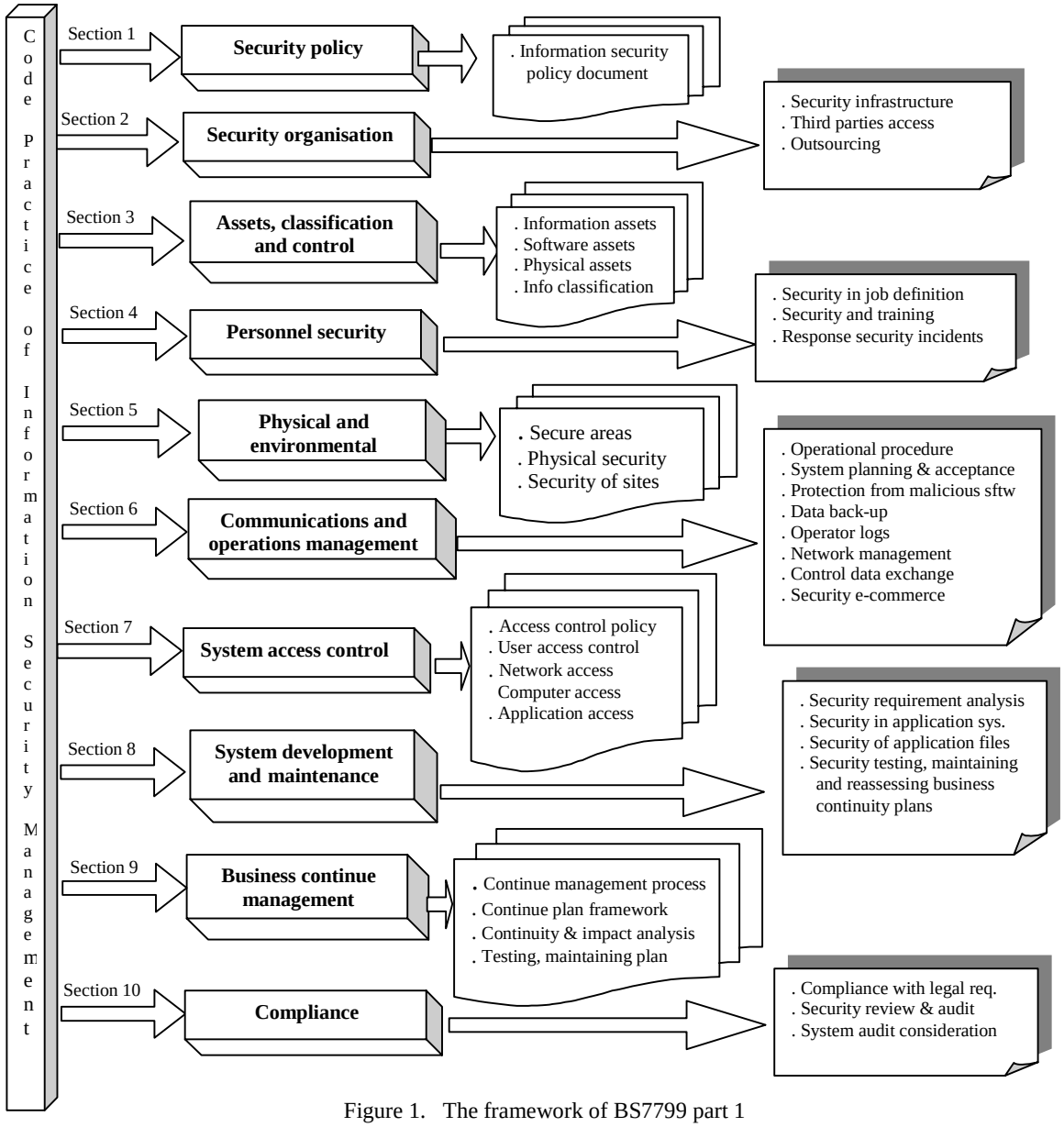

Figure 1. The framework of BS7799 part 1

(5) ***Physical and environmental security:*** Physical and environment security is to prevent unauthorised access and damage to IT services. Physical security has been considered by most of organisations. Information security management is heavily dependent on the safekeeping of the hardware infrastructure, which hosts that information.

(6) ***Computer and network management:*** The objective of computer and network management is to ensure the correct and secure operation of computer and network facilities, to minimise the risks of system failure and to maintain the integrity and availability of IT service. This is one of the largest sections in the standard and reflects the importance of good management of the computer and network by those responsible for the task.

A range of controls is required to achieve and maintain security in computer network. In particular, the following items should be addressed:

- operation responsibility for networks should be separated from computer operations;
- Responsibilities and procedures for the management of remote equipment should be established;
- Special controls should be established, if necessary, to safeguard the confidentiality and integrity of data passing over public networks, and to protect the connected systems.
- Management activities should be closely co-ordinated.

(7) ***System access control:*** Access control is about making information available to the right people in a secure way. System access can be controlled in a number of ways using hardware or software. This section of the standard includes: limited services, enforced path, user authentication, node authentication, remote diagnostic port protection, segregation in networks, network connection control, network routing control and security of network services.

(8) ***System development and maintenance:*** It is essential for those companies who are able to commission or design their own systems and applications to take every opportunity to make those systems fail-safe by the use of in-built controls. The recommendation areas of concern are:

- Security requirements of systems;
- Security in application systems;
- Security of application system files
- Security in development and support environments.

This section is intended primarily as a guide to the technical team and for the advice of the development companies.

(9) ***Business continuity planning:*** It is available to protect critical business processes from the effects of major failures and disasters. The recommendations of this section of the standard include:

- The business continue management process;
- Business continuity and impact analysis;
- Writing and implementing the continuity plan;
- Business continuity planning framework;
- Testing, maintaining and re-assessing business continuity plans.

The clear disaster recovery planning and processes will require the IT department to play a major role in replacing lost or damaged systems and infrastructure.

(10) ***Compliance:*** It provides guidelines on the potential internal and external regulatory information security obligations of organisation. The recommendations of this section are:

- Compliance with legal requirements;
- Control of proprietary software copying;
- Safeguarding of organisational records;
- Data protection;
- Prevention of misuse of IT facilities;
- Compliance with security policy;
- Technical compliance checking;
- System audit controls;

Compliance with security policy to be regularly monitored throughout an organisation and all elements of information security management analysed periodically.

2.2 BS7799 part 2: The Management Standard

BS7799 Part 2 is a standard specification for an information security management system (ISMS), it defines a six-step process to instruct organisation how to build an ISMS, the following are the major steps toward BS7799 compliance.

The first step of information security management is to define the information security policy, that identifies what information is important and why.

The second step is to define the scope of the ISMS, define the scope of management concerns. Organisations may need to regard all of their information systems and their external interfaces to define the clear scope of the ISMS.

The third step is to determine and assess the potential risks. It has been recommended to consider every possible risk at an early stage. For example: complexities of technology risks, business forces in terms of advancing technology and enterprise, people risks, as well as the ugly side of industrial espionage and information warfare.

After threats, vulnerabilities, and risk impacts have been defined, how to manage risks will be carried out at step 4. It includes technology management, people management, administrative procedures, and physical management.

The step 5 is to select control objectives and controls to be implemented. Different organisations may give the additional controls based on their own structures, the additional controls may not in BS7799. The step 6 is to prepare statement of applicability and an effective continuity plan. An effective continuity plan is helpful for any organisations. The selected control objectives and controls, and the reasons for their selection should be documented in the statement of applicability.

The above six steps can be adjusted by different kinds of organisations and should be reviewed at appropriately defined intervals as required.

3. The Further Concerns and Process Improvement in BS7799

BS7799 information security management standard has its advantages and disadvantages. The major advantage of BS7799 is that it is a published standard and will be probably from the basis of a new ISO standard in the same way that BS5750 became the basis of ISO 9000.

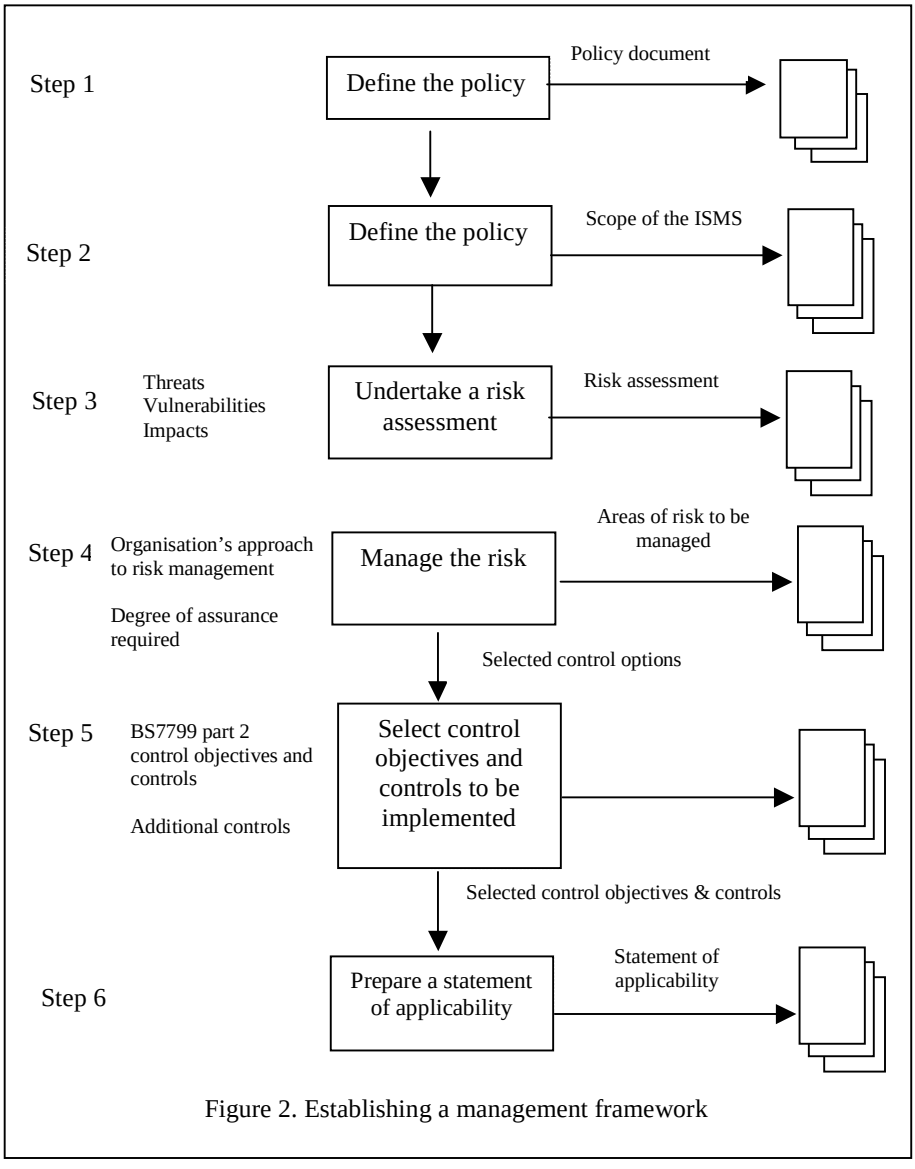

Figure 2. Establishing a management framework

The major disadvantage of BS7799 is that it will blindly adopted by a number of people and forced onto others as some form of panacea when in fact it becomes a placebo or just a source of significant revenue for an army of consultants. Following are some more considerations

- The BS7799 practice code does not address the major threats to information, such as theft of copies or misrepresentation.

- The BS7799 practice code on network access control does not mention cryptography. The code is briefly discusses cryptography, but only in a section on developing and maintaining application systems.

4. Survey Results

4.1 Critical Success Factors

Based on the methodology of BS7799 and the survey results which have been carried out by the Southampton Institute incorporate with British Computer Society, the following factors are often critical to the successful implementation of information security within an organisation.

- Security objectives and activities being based on business objectives and requirements, and led by business management;
- Visible support and commitment from top management;
- A good understanding of the security risks, both threats and vulnerabilities, to organisation assets and of the level of security inside the organisation, which should be based on the value and importance of the assets;
- Effective marketing of security to all managers and employees;
- Distribution of comprehensive guidance on information security policy and standards to all employees and contractors
- Make a flexible security policy, the security policy should be review or change it according to different period time and organisation's business focus.
- A comprehensive and balanced system of measurement which is used to evaluate performance in information security management and feedback suggestions for improvement.

4.2 The Survey Results of the Most Important Security Processes

Most of software houses, E-business, and financial organisations can only focus on a few security improvement activities at a time. It is difficult to cover the whole processes in small and medium organisation at same time. The survey analysed clear priorities, which provide guidance for selecting those few important activities that will be most helpful if implemented immediately. The survey results show that virus check, server database backup and clear security policies are high priority processes. Security tool usage, evaluation, and audit are also considered as affective security management processes.

4.3 Further Concerns from Developers, Users, and Managers

- *Human factors*

There has been a growing recognition in recent years that one of the important factors for information security management is the human factor.

When discussed with managers and directors, they considered more about human factor on organisation's sensitive database. As some employees may have a access right to view or change customer's database, this is a potential risk. They would like to try some security management tools to avoid this kind of risk at an earlier stage.

Some managers also highlighted that additional professional Internet security staff will be needed in next few years.

- *Virus protection*

According to survey, viruses and internal attacks pose as the greatest threats to network security that result in financial loss. Currently there are over 17,000 known virus. The great cause for alarm are the over 300 new viruses being discover every month. And even estimated 10 new viruses are released on the Internet every day.

- *Security tool usage*

Security automated tools can be used to prevent, find and fix problems. So far, developers are developing different kinds of tools, but some users feel it is difficult to identify which kinds of tools are suitable for their organisations. They suggested that it would be more helpful if some organisations can evaluate the existing security management tools and give some suggestions to users.

5. Conclusions

E-commerce needs a smarter approach to security, this paper presents the British security management standard BS7799 and discussed the framework of the security models. The methodology of the BS7799 approach has been analysed and a possible extension of information security management model is indicated.

The key features of BS7799 has been analysed, it shows that the most effective way of providing information security is to use a structured approach based upon organisation's specific requirements. It will ensure that organisation concentrate on the important areas.

A case study is being carried to investigate the best security management process practice and identify some of the specific problems appeared in the E-business security management areas. The survey results show that virus check, human factor, server database backup and clear security policy are high priority processes.

The BS7799 methodology is being used in both UK and non-UK organisations. The BS7799 intends to provide organisations with a quicker way to understand the methodology of the existing information security models, and to benefit managers with guidelines in selecting a suitable model while initiating an improvement programme in information security management.

Acknowledgements

The authors would like to acknowledge the support of British Standard Institute. This paper makes reference to the BS7799 related standard, we wish to thank the referees for their valuable comments in information security management area.

References

1. Brian Doswell, *Managing information security – Achieving BS7799*, 1998.

2. Ian Johnston, *BS7799 is like any standard – good and bad*, http://www.infowar.co.uk/white2.hml.

3. Keith Buzzard, *Computer security- what should you spend your money on?* Computer and Security Journal, 1999.

4. Lam Kwok, *Information security management and modelling, Information management and computer security*, 1999.

5. British Standards Institute, *BS7799: Code of practice for information security management*, 1995.

6. Bill Hancock, *Security View*, Computer and Security Journal 1999.

7. Ted Humphreys, *The New BS 7799*, XiSEC Consultants Ltd, April 1999.

8. *BS7799 part 2: Information security management, specification for information security management system. British Standard Institute*, 1998.

9. David Brewer, *Guaranteeing Security Transactions*, E-business Journal, published by Winthrop.

10. Mark Dixon, *The addressing of security regarding E-commerce*, Internal Report, 1999, UK.

11. Haiwen Li, Margaret Ross, Graham King, Geoff Staples, *A study of information security management and the potential use of BS7799 in various types of organisations*, Proceeding of INSPIRE'99, pp135-145, Crete, 1999.

12. Haiwen Li, Margaret Ross, Graham King, Geoff Staples, *Reducing risks through process improvement in rapidly changing business and E-commerce environments*, Proceeding of SQM'2000, pp131-142, Greenwich, 2000.

13. Haiwen Li, Margaret Ross, Graham King, Geoff Staples, *Process improvement approaches in a large software development organisation*, Proceeding of SQM'99 conference, pp103-116, UK. 1999.